REMARKS

In response to the Office Action mailed on July 18, 2007, Applicant(s) respectfully request(s) reconsideration. Claims 1-45 are now pending in this Application. Claims 1, 19 and 42-44 are independent claims and the remaining claims are dependent claims. In this Amendment, claim 44 has been amended and claim 45 has been added. Applicant(s) believe that the claim(s) as presented are in condition for allowance. A notice to this affect is respectfully requested.

Rejections under 35 U.S.C. § 112

Claim 44 stands rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular the Office Action at page 2 states that claim 44 use of the term "said ephemerizer" lacks sufficient antecedent basis. The claim has been amended to provide the correct antecedent basis.

Withdrawal of the rejection is respectfully requested.

Rejections under 35 U.S.C. § 102

Claims 1-44 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Perlman, U.S. Patent No. 6,363,480. The Applicant respectfully disagrees and traverses the rejection with and argument. Perlman discusses a system for ensuring that data can only decrypted for a finite period of time.

On page 3 of the Office Action, it is stated that Perlman, column 8 lines 18-31 and column 7, lines 23-43 teach "decrypting said blinded and encrypted message using an ephemeral decryption key of said ephemeral key pair to form a blinded message," as in claim 1. Perlman as cited does not teach decrypting a message that has been blinded and encrypted. Perlman, column 8 lines 18-31 states

> Upon receipt of the message from Party A, at step 106, Party B sends the doubly encrypted symmetric key to the ephemerizer indicated within the message.

> At step 108, the ephemerizer applies the appropriate ephemeral decryption key **to the doubly encrypted symmetric key**, for example using a private key from an ephemeral key pair also including the public key used as the ephemeral encryption key for the message. **The result of this decryption is a copy of the symmetric key still encrypted by the encryption key of Party B**. The ephemerizer passes this still encrypted symmetric key back to Party B, which then **uses its own decryption key to complete decrypting the symmetric key at step 108**. Party B uses the completely decrypted symmetric key to decrypt the body of the message. [Emphasis added]

Thus, what is discussed is the decryption of a symmetric key, not the decryption of a message that is also further blinded.

On page 3 of the Office Action, it is stated that Perlman, column 8 lines, 28-32 teach "communicating said blinded message to said first node." The cited text does not teach communicating the blinded message. The cited text quoted above, merely states that a symmetric key is communicated back to the node. Thus, Perlman discusses communicating the symmetric key, not the message that has been decrypted but still remains blinded.

Claims 19 and 42-44 teach similar features as discussed above. For at least the reasons discussed above, claims 1 and 42-44 and the claims dependent therefrom are patentably distinguishable form Perlman.

Claims 2 and 3 are patentable as being dependent from otherwise allowable claim 1. Further, nothing as cited in Perlman teaches or suggests that the ephemeral key ID is a associate with a RSA public and private key pair or Diffie-Hellman key pair as required in claims 2 and 3 respectively.

Claims 11 and 12 are patentable as being dependent from otherwise patentable independent claims. For at least the reasons stated above, the cited art failing to teach or suggest "said ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are an ephemeral RSA public key and corresponding private key, respectively," as in claim 11 or "the ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are Diffie-Hellman public and private keys, respectively," as in claim 12.

As regards claims 25-30, the Action states that Perlman column 5 lines 10-22 teach the features of these claims. The cited text does not teach "said blinding function, z, is a number R having an inverse R.sup.-1 that satisfies R*R.sup.-1=1 mod n and wherein said blinding step includes the step of forming the first blinded and encrypted message as the product (R.sup.e*M.sup.e mod n) where (M.sup.e mod n) is said message M encrypted using said ephemeral public encryption key," as in claim 27. Likewise the features of claims 25, 26 and 28-30 are like wise not taught or suggest by the cited text.

As regards claims 31-34, it is stated in the Office Action at page 6, that "encryption using public/private key pairs, which is inherently implied in, Perlman, column 5, lines 10-19." The Applicant respectfully disagrees. Nothing as cited discloses "said ephemeral public key is a Diffie-Hellman public key of the form g.sup.x mod p; selecting a blinding number y having an inverse blinding number y.sup.-1 that satisfies y*y.sup.-1=1 mod p-1; raising said public key g.sup.x mod p to the power y to obtain g.sup.xy mod p; raising g to the power y to form g.sup.y mod p; encrypting said message M using g.sup.xy mod p to form an encrypted message of the form {M}g.sup.xy mod p; storing a copy of said encrypted message {M}g.sup.xy mod p; and storing a copy of g.sup.y mod p," as in claim 31 or "selecting a blinding number, w having an inverse blinding function w.sup.-1 that satisfies w*w.sup.-1=1 mod p-1; raising said ephemeral public key g.sup.x mod p to the power w to obtain g.sup.yw mod p; forwarding g.sup.yw mod to said decryption agent; receiving g.sup.xyw mod p from said decryption agent; raising g.sup.xyw mod p to the inverse blinding number, w.sup.-1, to form g.sup.xy mod p; and decrypting said encrypted message {M}g.sup.xy mod p using g.sup.xy mod p to obtain said message M," as in claim 32. For at least the reasons stated above, claims 31-34 are patentably distinguishable from Perlman.

Withdrawal of the rejections is respectfully requested.

New Claim

Claim 45 is new. Support for the new claim found in claim 28. The cited art failing to teach where the decryption of the blinded and encrypted message is performed by raising the product ((R.sup.e*M.sup.e) mod n) to the power d mod n,

forming $((R.sup.e * M.sup.e)\ mod\ n)).sup.d\ mod\ n$ to form a first blinded message $R*M$ mod n. Applicants submit that the no new matter has been added by the addition of claim 45.
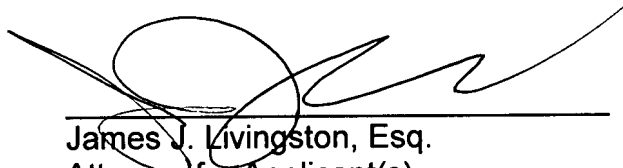
<div align="center">Summary</div>

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,

James J. Livingston, Esq.
Attorney for Applicant(s)
Registration No.: 55,394
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: SUN06-38(P9238)

Dated: September 25, 2007